Lecture 20

Dec 01, 2025

Quantum Error Correction.

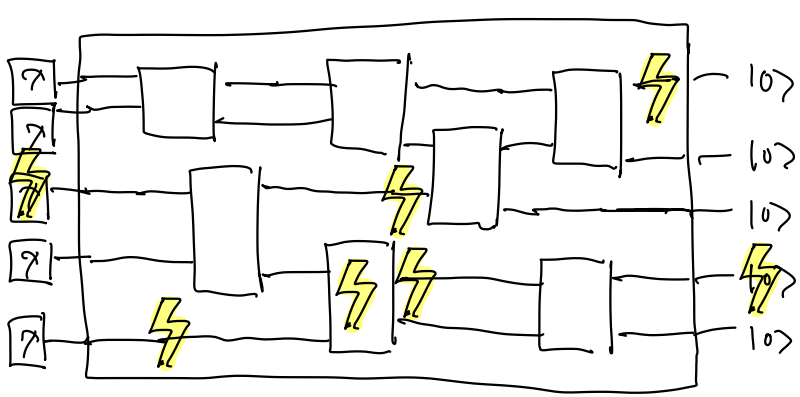
Until known, we have talked about perfect application of gates and perfect initializations of q. states.

What if that is not the case?

Error-correction gives a theory of how to recover information in the presence of noise.

Biggest blocks to our construction of large scale q. computers.

Quantum computation is more susceptible to noise than classical computation.



Errors can occur in any component...

How do we correct.

(1) A theory of correction for static q. information.

No computation occuring, just errors.

Run a sequence of corrections to return information back to original.

Quantum analog of reliable data storage.

Classical: CDs, SSDs, Harddrives, Pen and Paper

(2) Correction interspersed with computation

Called Fault-Tolerance and will be covered in Lecture 20 by guest lecturer Michael Beverland.

How do we correct classical information?

Theory: Rich. Practice: Redundancy.

Wifi/3G/4G : LDPC codes

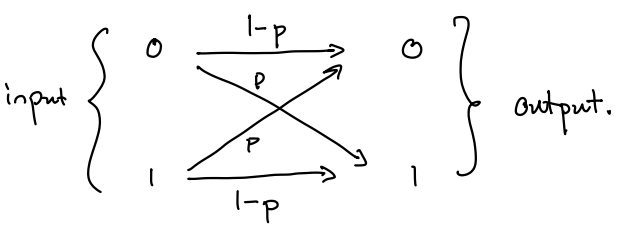
CD-Rom: Reed-Solomon codes

Computation: Run it thrice and take majority votes.

Reasonable because a classical bit in a modern transmitter incurs an error with $pr < 10^{-16}$.

To analyse error-correction (theoretically), we first need a model for error.

Simplest model bit flip channel.



$$\rho \longmapsto \mathcal{E}(\rho) = p \cdot X\rho X + (1-p)\,\rho.$$

Notion holds for quantum also.

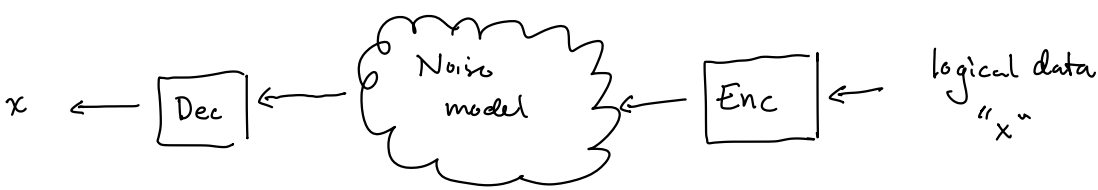
High level: A channel is a map from density matrices to density matrices consistent with q. mechanics axioms.

Bit flip on each bit:

$\mathcal{L}(\mathbb{C}^{2^n}) \ni \rho \longmapsto \mathcal{E}^{\otimes n}(\rho)$.

$\Pr[\text{no bit gets flipped}] = (1-p)^n \longrightarrow 0$ as $n \longrightarrow \infty$.

General procedure.



Easiest classical example: Repetition code.

$\overline{0} := \text{Enc}(0) = 0 \ldots\ldots 0$

$\overline{1} := \text{Enc}(1) = \underbrace{1 \ldots\ldots 1}_{n \text{ times}}$.

Assume $p < \frac{1}{2}$.

$$Dec(y) = \begin{cases} 0 & \text{if } |y| < \frac{n}{2} \\ 1 & \text{if } |y| > \frac{n}{2} \end{cases}.$$

$$\Pr_{\text{error}}\left[\text{decoding is wrong}\right] = \Pr_{\text{error}}\left[\geq \frac{n}{2} \text{ bits flipped}\right] \leq e^{-\delta(n)}$$

The 3 troubles of quantum error correction.

(1) Infinite collection of possible errors even just on one qubit.

(2) No-cloning theorem.

There is no unitary mapping $|0\rangle \mapsto |0\rangle|0\rangle$ and $|+\rangle \mapsto |+\rangle|+\rangle$

Therefore quantum repetition code doesn't make sense.

(3) Measurements destroy quantum info.

How do we correct when measurement is perturbative?

Today: Shor's 9 qubit code + theory of EC.

Let's correct first for a specific subset of errors:

Single qubit X (bit flip), Z (phase flip), and XZ (bit + phase)

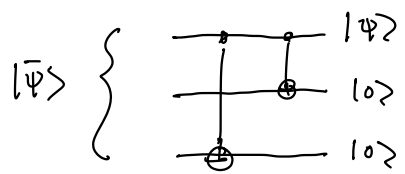
To correct just bit flip errors, appeal to classical intuition.

map $|0\rangle \longmapsto |000\rangle$

$|1\rangle \longmapsto |111\rangle$

} Does not violates no cloning as we copy in 1 basis

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longmapsto |\bar{\psi}\rangle = \text{Enc}|\psi\rangle = \alpha|000\rangle + \beta|111\rangle.$

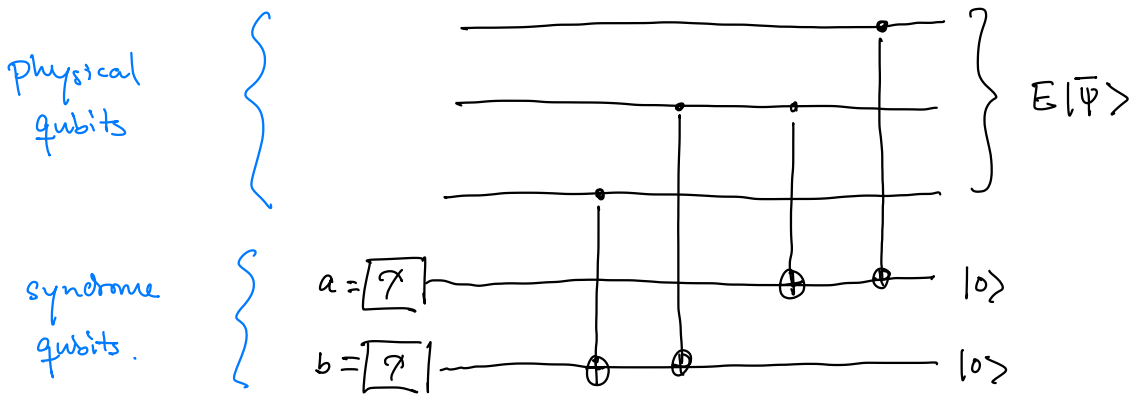


Say error occurs on middle qubit.

$$E|\bar{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle.$$

Measuring would destroy superposition.

Instead, we compute error-syndromes and measure these.



If run on $|x,y,z\rangle$, then $a = x \oplus y$, $b = y \oplus z$.

$$a \oplus b = x \oplus z.$$

By linearity, when run on $E|\bar{\psi}\rangle = \alpha|0\,1\,0\rangle + \beta|1\,0\,1\rangle$

we get

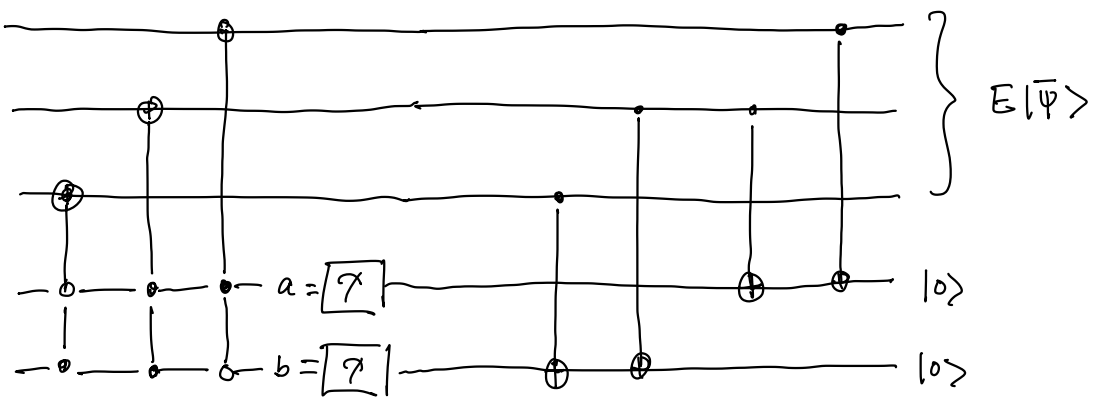
$$\alpha|0\,1\,0\rangle|1\,1\rangle + \beta|1\,0\,1\rangle|1\,1\rangle$$

$$= \left(E|\bar{\psi}\rangle\right) \otimes |1\,1\,1\rangle.$$

$|1\,1\,1\rangle$ → syndrome

What happens for other bit flip errors?

Error	a	b
no error	0	0
1st qubit	1	0
2nd qubit	1	1
3rd qubit	0	1



After correction, we can discard the syndrome qubits (they are now unentangled by measurement).

$$\text{Dec} = \text{Enc}^{-1} \circ \text{Correction}$$

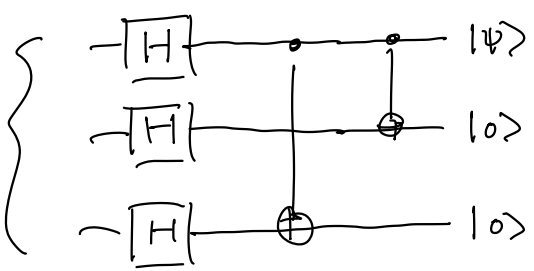
Correcting only phase errors:

Note $HZH = X$. Phase errors are bit flip errors in a different basis.

$$|0\rangle \longmapsto |+++\rangle$$
$$|1\rangle \longmapsto |---\rangle.$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longmapsto |\bar{\psi}\rangle = \alpha|+++\rangle + \beta|---\rangle.$$

$|\bar{\psi}\rangle$

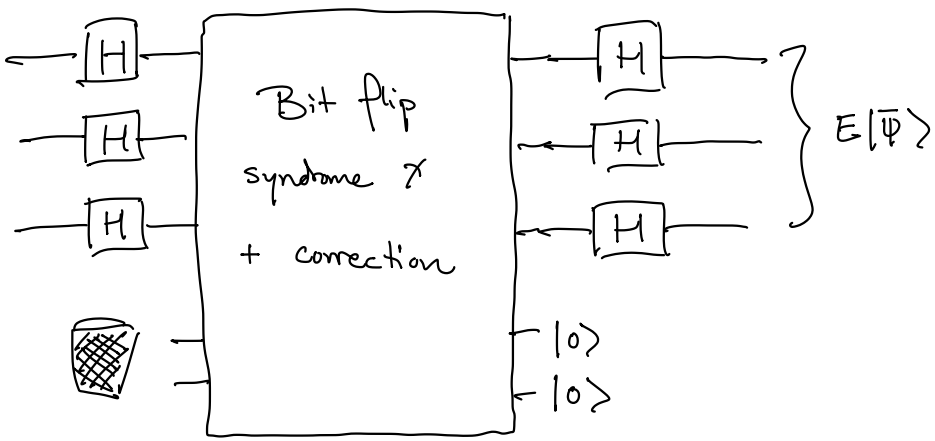


Z error on 3rd qubit. Then

$$\alpha|+++\rangle + \beta|---\rangle \xrightarrow{Z_3} \underbrace{\alpha|++-\rangle + \beta|--+\rangle}.$$

$$= H^{\otimes 3}\alpha|001\rangle + \beta|110\rangle.$$

So correction circuit is easy to concoct.



Note if we encode in phase flip code but X_1 occurs then

$$\alpha|+++\rangle + \beta|---\rangle \xrightarrow{X_1} \alpha|+++\rangle - \beta|---\rangle$$

New states will have syndrome $(0,0)$ for phase flip code and corresponds to applying $\bar{Z}$ on underlying logical information.

Same with phase flip for bit flip encoding.

How do we combine to get both error corrections?

Ans: Encode in one code and then in the other.

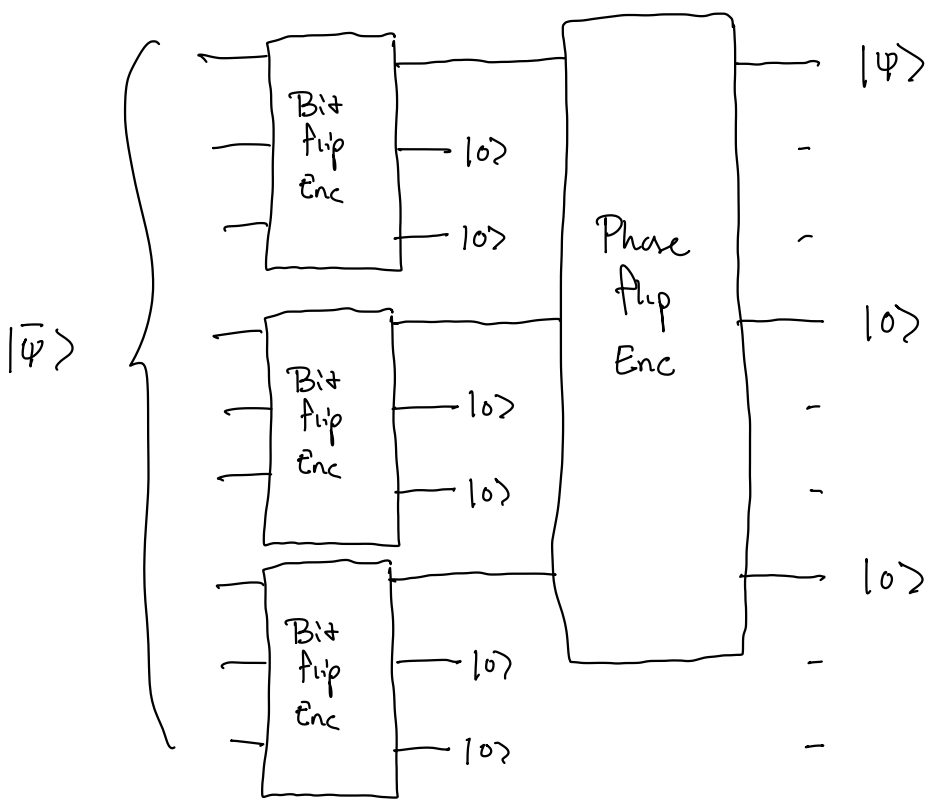
$$|0\rangle \longmapsto |+\rangle^{\otimes 3} \longmapsto \frac{1}{\sqrt{8}}\left(|000\rangle + |111\rangle\right)^{\otimes 3}$$

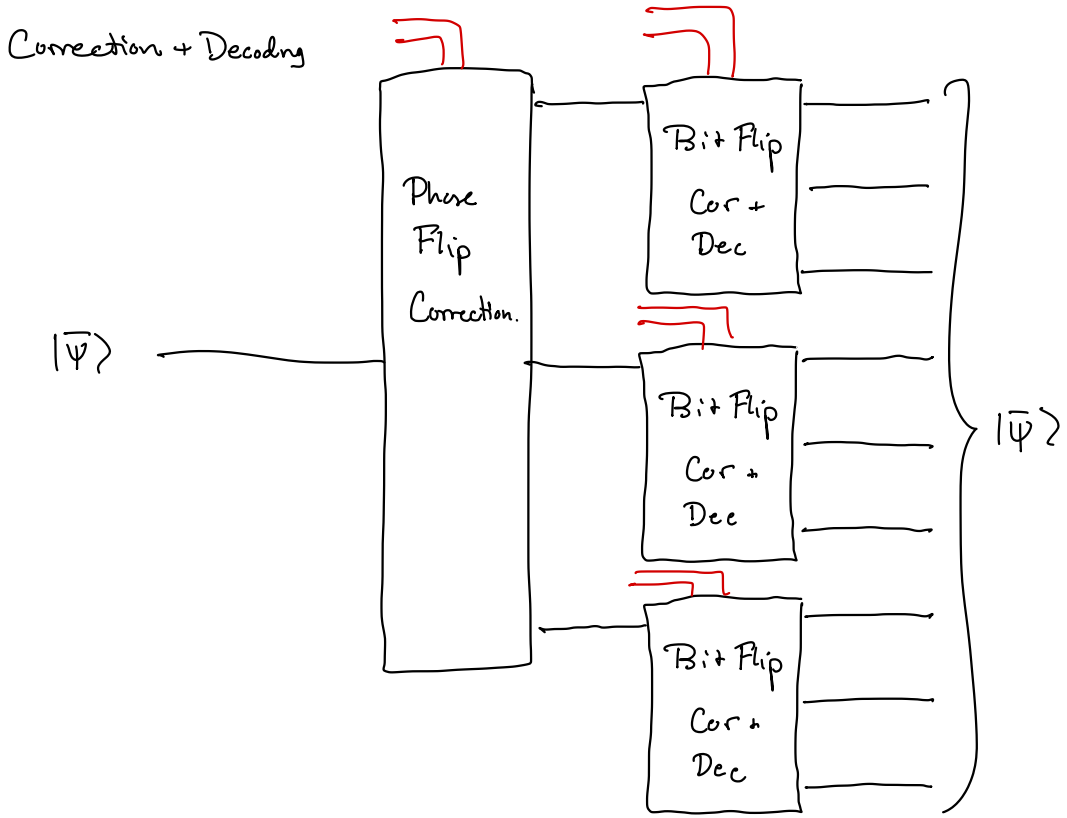
$$|1\rangle \longmapsto |-\rangle^{\otimes 3} \longmapsto \frac{1}{\sqrt{8}}\left(|000\rangle - |111\rangle\right)^{\otimes 3}$$

Could have also done in the other order

↑ But has different correction operators.

Encoding:





This corrects any 1 bit flip error per triple and 1 phase flip error. To correct bit + phase flip error in the same qubit, both syndromes check.

Fact. Every Hermitian $H \in \mathbb{C}^{2\times 2}$ equals

$$H = \alpha \mathbb{1} + \beta X + \gamma(XZ) + \delta Z.$$

Next lectures:

① What about infinite family of errors?

(Rough answer: Pauli errors form a basis for all errors)

② Can we correct without decoding? (Yes)

③ How do we encode more than 1 qubit of logical information?

Is there a general theory of why this is working?

A general theory of q. error correction.

(Slides as there are a lot of drawings)

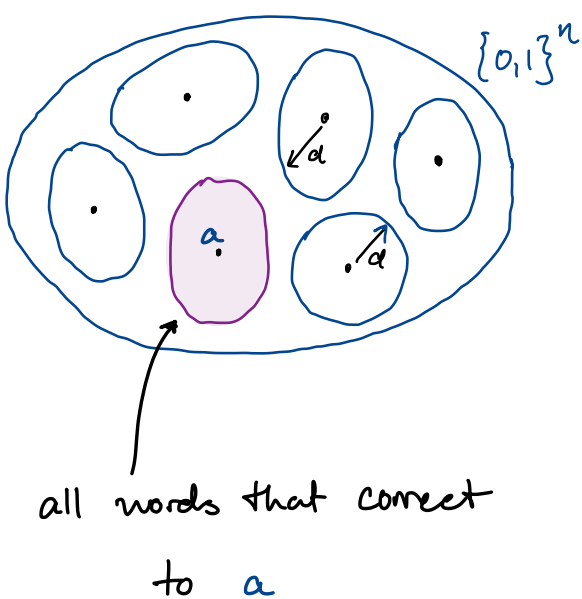
Part 2 (of Lec 17)

An (abridged) theory of classical error correction.

A subset $C \subseteq \{0,1\}^n$ is a code encoding k bits into n bits if $|C| = 2^k$.

The distance of the code is $d = \min_{\substack{x,y \in C \\ x \neq y}} d_H(x,y)$

the min number of bits required required to flip some $x \in C$ to $y \in C$. A code of distance d can correct $\lfloor \frac{d-1}{2} \rfloor$ errors.



Typically, when people talk about classical error correction they are talking about linear codes.

$k = \dim C$ and $C = \ker A$ ← check matrix.

Notation: $C = [n, k, d]$ code with locality ℓ if $C = \ker A$ with A being ℓ-row & ℓ-column sparse.

Ex. $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$. $Ax = 0$ equals

$$x_1 \oplus x_2 = x_2 \oplus x_3 = 0.$$

$C = [3, 1, 3]$ code.

$$d = \min_{\substack{x \neq y \\ x, y \in C}} d_H(x, y) = \min_{\substack{x \in C \\ x \neq 0}} |x|.$$